



Can my Google Admin account be
compromised over open wireless?

(B307)

COLLEGE OF
Saint Benedict  Saint John's
UNIVERSITY

Enik Pluimer - Network Administrator

Saint Joseph - Collegetown, MN

2 Campuses - 6 Miles Apart

Undergraduate Enrollment - 3,405

17,000 Switch Ports

1,100 Access Points

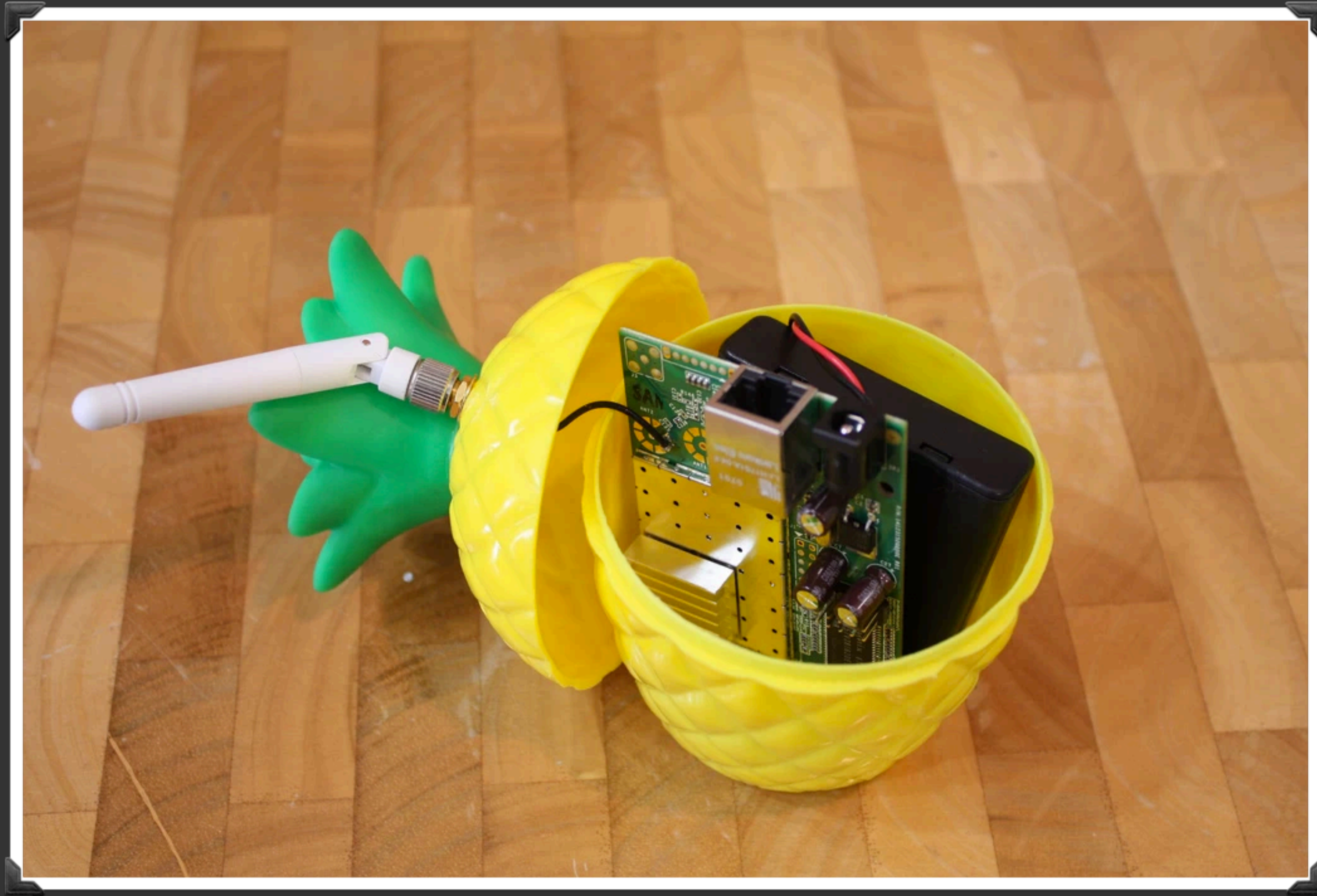


Google Admin: Compromised?





History





Dear Lamer,

You just got popped with some 0-day s**t.

Mess with the best and die like the rest. Should have just bought a t-shirt.

You're going to mess around with someone's Wi-Fi in Vegas at a f***ing hacker con? What the h*ll did you expect?

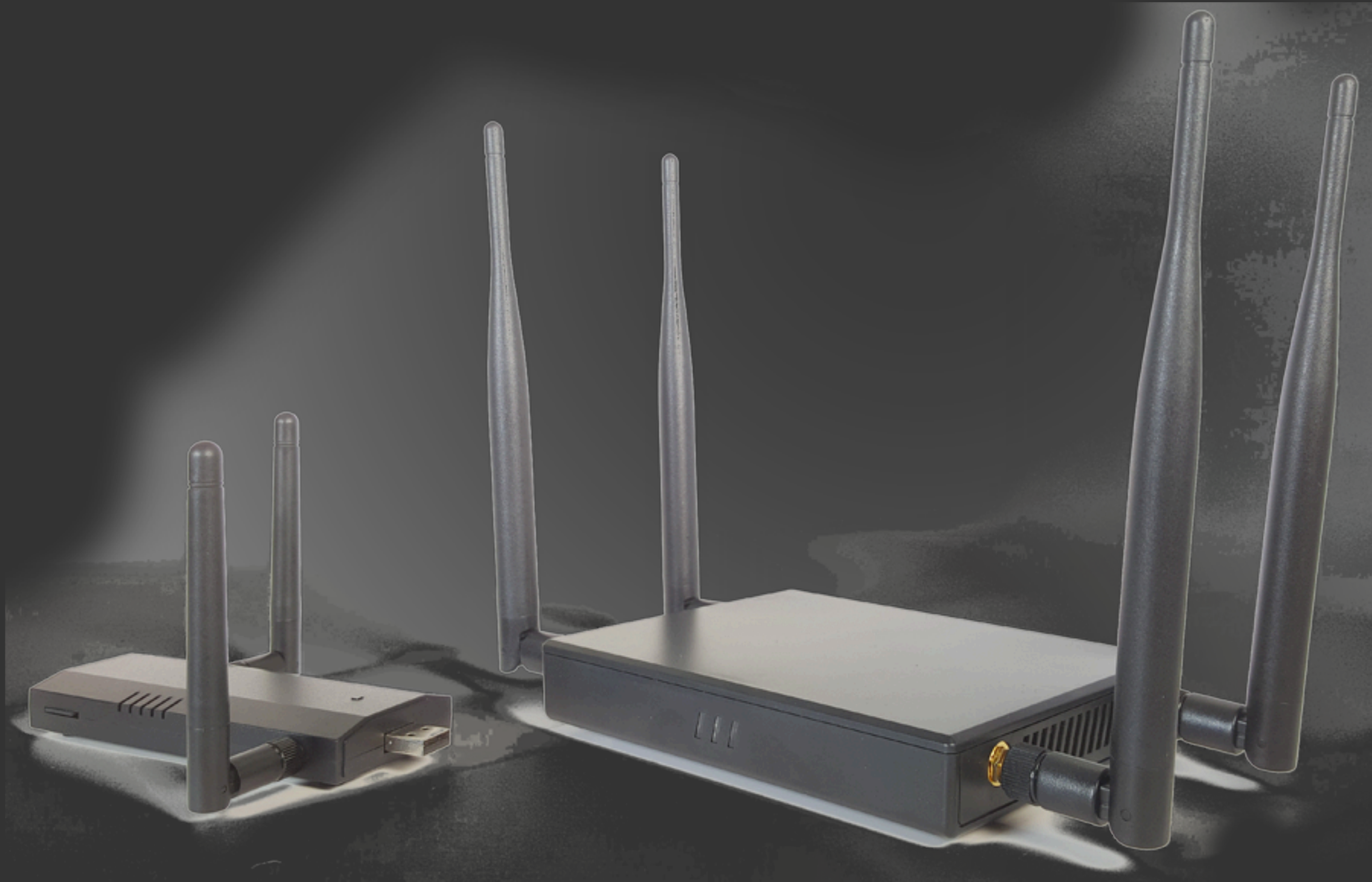
Your sh*t's all wrecked now. If you really are the bad*ss you're pretending to be, you ought to be able to fix it.

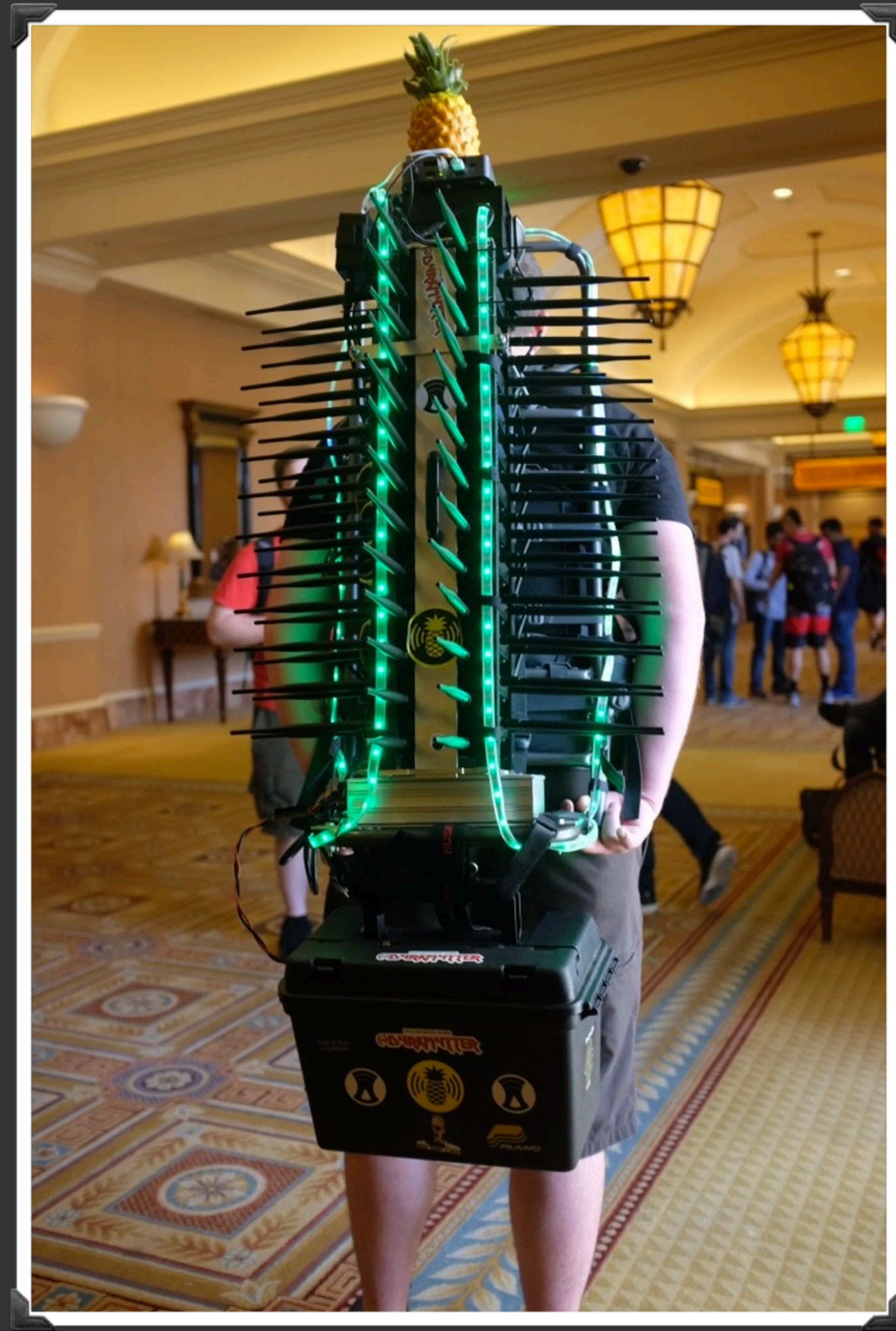
If you have no idea what is going on then I recommend you take this back to the Hak5 booth, ask for a refund, and stop sh***ing-up the Wi-Fi.

Read the f***ing code the next time you buy super elite skiddie hax0r gear. This s**t is criminally insecure.

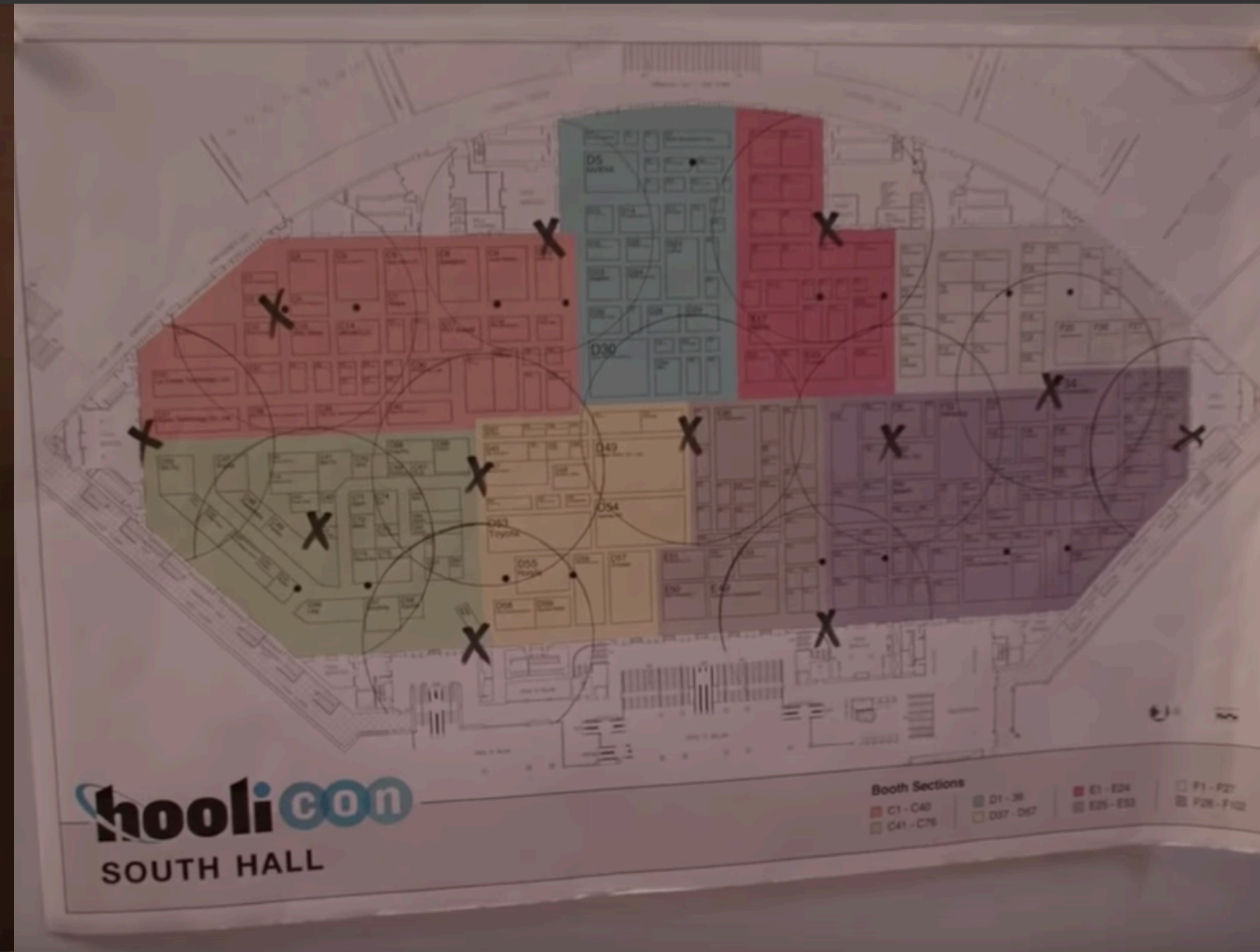
Sincerely,

@IHuntPineapples

















USB / DC / POE / Battery powered

USB Port - GPS, Ethernet, WiFi, Modems, Androids

Ethernet and Serial Ports

Micro SD Slot for storage

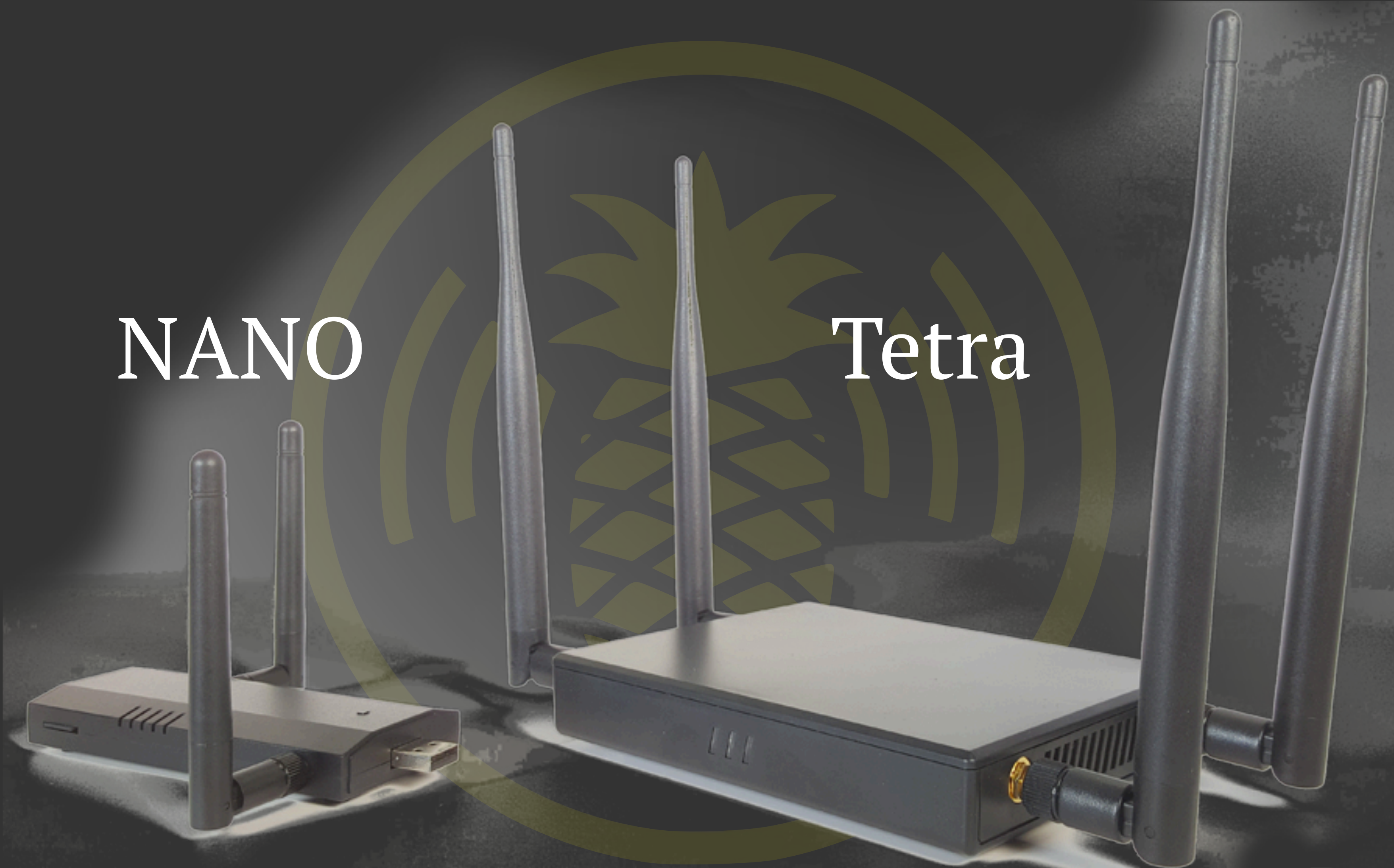
External antenna capability

Mobile auditing

Long term deployments

NANO

Tetra







PineAP: Rogue Access Point

Listens for your probe requests

Mimics your preferred networks

Auto connect devices

Known as Evil Twin attack

Evil Portal: Rogue Captive portal

Present users cloned versions of known sites

Harvest credentials

Potentially inject malware

Be annoying

DNSSpoof: Rogue DNS Server

Redirect users from trusted domain names

Present fake pages

Assists EvilPortal



SSL Split:
SSL/TLS Proxy
Forge Certificates
Decode Plaintext



NMAP: Port mapping utility

TCPDUMP: Packet capture utility

WPS: (Pushbutton Security) attacks

MDK3: Suite of wireless protocol attacks

Attacks:

Persistent and Targeted

Denial of Service

Wireless Security

Application Protocols

Social

Persistent:

Reverse SSH tunnel back to CNC

Collect data and patterns and be 'quiet'

Log data locally or to a remote server

Targeted:

Entice a single client with targeted methods

Reduce the chance of detection

Denial of Service:

Annoy people

Pick on a single MAC or everyone

Skip around on channels sending de-authentication

Jamming and Spamming: Randomroll, OccuPineapple

Wireless security:

MAC (Data Link) layer

Exploit on boarding features like WPS

Capture the 4-way handshake for offline cracking

New attack on WPA/WPA2 using PMKID

KRACK attack / forced nonce reuse

GPUHASH.me ^{BETA}

Tasks queue

Add new task

Get result











Verify WPA

Contact us

Hide queue

Tasks queued: **194** WPA processed: **100057** WPA cracked: **27.98/34.07%** Hashes processed: **4.79M** Hashes cracked: **33.96%** GPU cluster speed: **WPA: 7.76MH/s**

WPA: 941KH/s WPA: 702KH/s WPA: 1.10MH/s WPA WPA: 1.18MH/s WPA: 741KH/s WPA: 866KH/s WPA: 796KH/s WPA: 1.44MH/s IDLE IDLE

Task ID	Type	Description	Priority	Status	Time spent	Attack configuration
 2duT...	NTLM	[NetNTLMv2] Digests: 14, salts: 14	1	Waiting payment	-	Advanced search
 GZyV...	NTLM	[NetNTLMv1] Digests: 2, salts: 2	1	Waiting payment	-	Advanced search
N7U6...	WPA	-	1	Waiting payment	-	Basic search
 6LvX...	WPA	FASTWEB-DEK084	1	Waiting payment	-	10 HEX uppercase
 5NME...	WPA	WFM918	0	Waiting approval	-	Basic search
 A3xt...	WPA	WATASHI_2.4G	0	Waiting approval	-	Basic search
 91we...	WPA	Voice_Audit_Store	0	Waiting approval	-	Basic search
 38Dm...	WPA	true_home2G_Kb6	0	Waiting approval	-	Basic search
 99ng...	WPA	Nodu	0	Waiting approval	-	Basic search
 EB1B...	WPA	cpfm	0	Waiting approval	-	Basic search
 Bqt6...	WPA	CASPER CJ	0	Waiting approval	-	Basic search
 DBC9...	WPA	Brandt House2	0	Waiting approval	-	Basic search
 3hef...	WPA	BestNetWork	0	Waiting approval	-	Basic search
 9Hjz...	WPA	adwifiadmin	0	Waiting approval	-	Basic search

Application Protocols:

Degrade secure HTTPS sessions to plaintext HTTP

Harvest data from un-secure forms

Steal un-secure HTTP session cookies

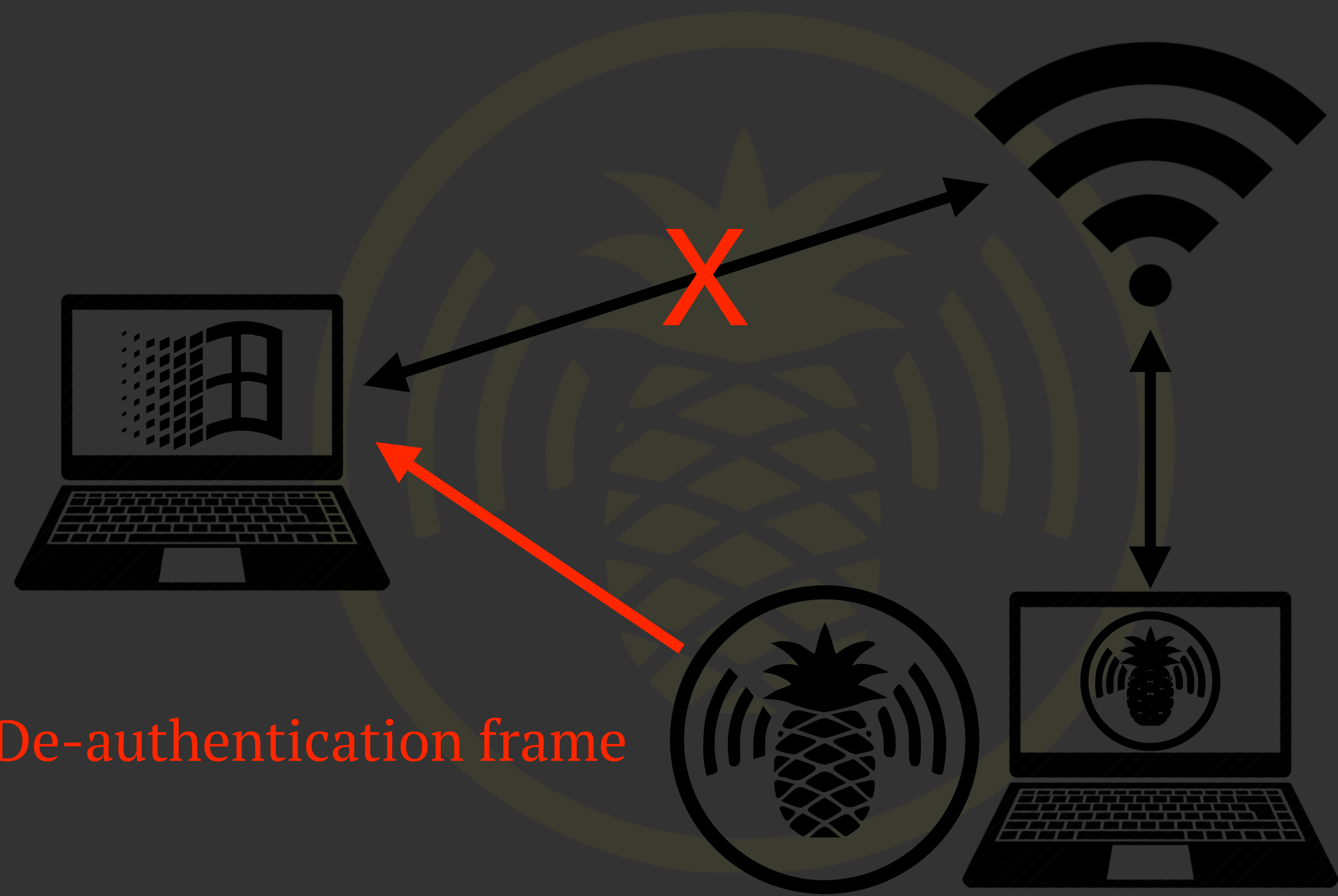
Steal session data and credentials from other apps



Social Attacks:
Manipulate user trust
Present fraudulent data
Install malicious payloads
Harvest data







De-authentication frame







User Mitigation:

Disable auto-connect

Don't use open networks

But if you do: Pay attention

Don't transmit sensitive data

Forget networks before leaving

Use VPN or cellular network

Application Mitigation:

Keep your Apps and browsers updated

Always use HTTPS

Be aware of cleartext forms

Use HSTS to prevent downgrade

HTTP session cookies vulnerable

Deploy Password Alert extension for Chrome

HTTPS Everywhere for Chrome

Infrastructure Mitigation:

Patch and update code often

Preferred encryption WPA2 EAP-TLS

Avoid open networks for your clients

Enforcement of security policies

Detect with WIPS:

Multiple SSID per MAC

Bridging of wired traffic

WPA3 and WPA3 Enhanced Open?

WPA2 - Enterprise EAP-TLS

WPA2 Enterprise EAP-PEAP

WPA2 - PPSK

WPA2- PSK

WPS and Open

Known networks are "scored" based on your actions. If you manually switch to an SSID, its score increases. If you manually disconnect from an SSID, its score decreases. "Most preferred" networks have higher scores.

If iOS finds multiple networks after evaluating the above criteria, iOS prioritizes SSIDs by security level and chooses one based on the following order:

	Network Category	Network Security
1	Private	EAP
2	Private	WPA
3	Private	WEP
4	Private	Unsecure/Open
5	Public	HS2.0/Passpoint
6	Public	EAP
7	Public	WPA
8	Public	WEP
9	Public	Unsecure/Open

If iOS finds multiple networks of identical category and security level, it chooses the SSID with the strongest received signal strength indication (RSSI). Learn more [about RSSI and wireless roaming for enterprise](#).



HSTS (HTTP Strict Transport Security) is an HTTP Header that tells a client (aka a browser) that it should only be allowed to connect with the site with a valid HTTPS certificate.

Server must follow HSTS protocols

Previous HTTPS session required within timeframe

Site owners can use HSTS to identify users without cookies

Cookies can be manipulated from sub-domains

HTTP Strict Transport Security

<https://www.chromium.org/hsts>

<https://hstspreload.org>

<https://badssl.com/>

<chrome://net-internals/#hsts>

When it comes to networking info sec, vigilance is key.

The most secure option
is to never use public Wi-Fi networks at all.

-Daniel Oberhaus

